UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,285	10/10/2000	John M. Hammer	05456.105008	4449

69151 7590 10/09/2007

KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA, GA 30309-3521

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
10/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mv

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/685,285
Filing Date: October 10, 2000
Appellant(s): HAMMER ET AL.

Steven P. Wigmore (Reg. No. 40,447) - KING & SPALDING LLP

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 7/6/2007 appealing from the Office action mailed 3/20/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows: claims 51-55 are now rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack, et al. (US 6,298,445) in view of Reps, et al. (US 6,070,190).

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,298,445	SHOSTACK, ET AL.	10-2001
6,453,345	TRCKA, ET AL.	9-2002
6,070,190	REPS, ET AL.	5-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-9 and 11-50, and 56-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack, et al. (US 6,298,445) in view of Trcka, et al. (US 6,453,345).

As per claim 1:

Shostack, et al. disclose a method for automatically creating a record for one or more security incidents and reactions thereto, comprising the steps of:

recording computer security incident information [col.2, lines 62-63 and col.13, lines 42-43] *[with at least one of a date and time stamp]*, the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network [col.4, lines 47-50 and col.5, lines 20-50] that occur prior to a computer security threat [col.7, lines 13-17] and an actual computer security threat; [col.4, lines 50-53]

classifying the computer security incident information; [col.9, lines 59-67]

automatically suggesting one or more computer security threat procedures based on a classification of the computer security incident information; [col.7, lines 25-35 and col.11, lines 52-54]

displaying the one or more suggested computer security threat procedures [col.12, lines 14-25 and 41-47], each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information; [col.6, lines 58]

[receiving a selection of a suggested computer security threat procedure from a user, the selection comprising one or more steps of the selected computer security threat procedure;]

executing the selected one or more steps of the procedure; [col.2, lines 54-56 and col.7, lines 56-57]

in response to executing the one or more steps of the selected computer security threat procedure, recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure [col.7, lines 25-27] [*with at least one of a date and time stamp; and*]

outputting a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure [col.13, lines 15-17 and 31-36], the identity of a user who selected the computer security threat procedure [col.9, lines 16-17 and 56-63], and at least one of a corresponding [*date and time stamp*].

Shostack discusses displaying the one or more suggested computer security threat procedures [col.12, lines 14-25 and 41-47], each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information [col.6, lines 58 and col.7, lines 25-27]. However, Shostack did not include a date and time stamp and receiving a selection of a suggested computer security threat procedure from a user.

Trcka, et al. discloses an invention that provides a network security and analysis system, which includes a variety of features for automatically and interactively monitoring and analyzing traffic (col.2, lines 11-15 and col.11, lines 1-4). Trcka utilizes archival recordings to evaluate security breaches and other anomalies (col.7, lines 49-50). The archival recordings can be used to perform a wide range of network analysis and restoration tasks that includes checking for newly discovered viruses and performing low-level analysis of network break-ins (col.2, lines 56-61). Trcka discusses the date/time stamp reflects the dates and times that the packets are transmitted on the network (col.15, lines 55-57). Thus, preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12). Further, the claimed "receiving a selection of a suggested computer

security threat procedure from a user, the selection comprising one or more steps of the selected computer security threat procedure", broadly limits a computer security threat procedure that is suggested from a user. This does not limit or define what considers a procedure and security threat involves that can be selected or suggested from a user. The claimed subject matter merely suggests as long as the procedure is computer security threat related. For instance, a selection of a suggest computer security threat procedure from a user can broadly be given in light as security configurations to help prevent or monitor security threats, allowing or not allowing particular traffic or incoming packets, a solution to solve security threat, or specifying types of transactions or filtering parameters. Thus, the following will explain and incorporate these examples found in Trcka. Trcka includes various software routines for monitoring, filtering, searching, and manipulating traffic data and interactive analysis applications which provide functionality for allowing users to interactively analyze and process traffic data (col.12, lines 49-52). In addition, the Automated Monitor application uses known data processing techniques (virus checking, transaction, monitoring, etc.) to automatically check for and track suspect network events and one configuration option, a user can enable or disable various visual and audible event alarms (col.17, lines 24-32). The user can configure to alert the user when critical limits are exceeded on the network, generate log file of specific types of events, run analysis applications and perform other interactive actions in the foreground (col.17, lines 35-42). The analysis applications provide various functionality for allowing users to interactively perform non-real-time or off line analyses of pre-recorded raw traffic data (col.17, lines 44-50). This shows the user having the

ability to interact, which obviously gives instructions to enable a selection of suggested computer security threat procedures in order to receive a selection of suggested computer security threat procedures from a user (col.12, lines 49-52 and col.20, lines 1-17). In addition, Trcka discloses the GUI allows the user to specify the type or types of transactions that are loaded into the databases and/or routed directly to the analysis applications. The types of filtering parameters that can be set by the user include network address, traffic type, packet type, user ID, and packet transaction sequence (col.18, lines 1-14). Trcka discloses the user able to initiate searches of the traffic data at various levels of resolution and search for all packets containing the particular set of source and destination address or for all packets transmitted during a particular time window (col.18, lines 15-52).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the computer security threat procedure computer based on classification of security incident information as taught by Shostack with the teaching of allowing the user to interactively perform analyses of traffic data such that the receiving a selection of a suggested computer security threat procedure from a user as taught by Trcka because this allows the user to specify computer security threats procedures such as types of transactions that are loaded into the databases (col.18, lines 1-2 and 40-44), configure to generate a log file of specific types of events (col.17, lines 38-50), and traffic analysis of the particular packets (col.12, lines 49-52 and col.20, lines 1-17).

Additionally, it would have been obvious to combine the teaching of recording computer security incident information and the computer security threat procedure as taught by Shostack with at least one of a date and time stamp as taught by Trcka because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

As per claim 2: see Trcka on col.7, lines 1-3; discussing an unmodifiable permanent database.

As per claim 3: see Shostack on col.11, lines 5-17 and col.13, lines 50-55; discussing the step of recording the results of the executed computer security threat procedure with a digital signature to enable detection of any modification of the recorded results, whereby integrity of the recorded results can be monitored.

As per claim 4: see Shostack on col.7, lines 55-60 and col.10, lines 50-54; discusses extracting the information from the results of an executed computer security threat procedure.

As per claim 5: see Shostack on col.7, lines 14-27 and col.10, lines 50-54; discusses describing a computer security incident with said extraction information.

As per claim 6: see Shostack on col.12, lines 14-25 and 41-47; discussing displaying information for a particular computer security incident to more than one user.

As per claim 7: see Shostack on col.13, lines 7-17; discusses prepopulating fields of a record of a first program module from a second program module.

As per claim 8: see Shostack on col.7, lines 10-29; discusses receiving security incident information from a first program module; processing the security incident

information with a second program module; and forwarding the processed computer security incident information from the second program module to a third program module.

As per claim 9: see Shostack on col.11, lines 52-54; discusses receiving a selection of a computer security threat procedure comprises automatically selecting a computer security threat procedure with a program module.

As per claim 10: Cancelled

As per claim 11: see Shostack on col.11, lines 52-54; discussing each steps are performed automatically by a program module.

As per claim 12: see Shostack on col.11, lines 52-54; discussing some steps are performed automatically by a program module.

As per claim 13: see Shostack on col.13, lines 7-17; discusses displaying reports comprising one or more computer security incidents.

As per claim 14: see Shostack on col.12, lines 46-47; discussing the results of an executed procedure comprises at least one of text, numbers, images, or formatted documents.

As per claim 15: see Shostack on col.7, lines 13-15; discusses predicting future actions of a source of a computer security incident.

As per claim 16: see Shostack on col.5, lines 21-61; discusses identifying the source of a computer security incident.

As per claim 17: see Shostack on col.6, lines 42-46; discusses sorting decoy or false security incidents from actual computer security incidents.

As per claim 18: see Shostack on col.7, lines 25-29 and col.11, lines 50-51; discusses linking a first computer security threat procedure to a second computer security threat procedure.

As per claim 19: see Shostack on col.12, lines 58-65; discusses determining the authorization level of a user.

As per claim 20: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47; discusses providing data to enable display of a computer security threat procedure further comprises the step of providing data for enabling display of one or more steps of a computer security threat procedure.

As per claim 21: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47; discusses providing data to enable display of a computer security threat response procedure; executing the computer security threat response procedure [col.7, lines 56-57]; and in response to executing the response computer security threat procedure, recording executed computer security threat response procedure information and results of the executed computer security threat response procedure [col.7, lines 25-27 and col.13, lines 15-17 and 31-36] with at least one of a date and time stamp (Trcka-col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57).

As per claim 22: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47; discusses providing data to enable display of a computer security threat investigation procedure; executing the computer security threat response procedure; and in response to executing computer security threat investigation procedure [col.7, lines 56-57]; and recording executed computer security threat response procedure

information and results of the executed computer security threat response procedure [col.7, lines 25-27 and col.13, lines 15-17 and 31-36] with at least one of a date and time stamp (Trcka-col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57).

As per claim 23: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47; discusses providing data to enable display of the computer security threat response procedure further comprises the step of providing data to enable display of one or more steps of the computer security threat response procedure.

As per claim 24: see Shostack on col.8, lines 63-67 and col.12, lines 14-25 and 41-47; discusses providing data to enable display of results of the executed computer security threat procedure.

As per claim 25: see Shostack on col.7, lines 24-29 and col.11, lines 50-54; discusses providing data to enable display of results of the executed computer security threat procedure.

As per claim 26: see Shostack on col.7, lines 24-29 and col.11, lines 50-54; discusses identifying an appropriate computer to execute a step in the computer security threat investigation procedure; and identifying an appropriate computer to execute a step in the computer security threat response procedure.

As per claim 27: see Shostack on col.10, lines 52-60 and Trcka on col.7, lines 60-63; discusses accessing a table comprising computer locations and step information; comparing a step to be executed with computer locations listed in the table; determining if a match exists between the step to be executed and the computer locations; and if

one or more matches exist, displaying the matching information or automatically selecting appropriate location.

As per claim 28: see Trcka on col.7, lines 60-63 and col.18, lines 1-14; discussing the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of a source of a computer security incident with the Internet address ranges of the table.

As per claim 29: see Trcka on col.15, lines 50-54; discusses providing data to enable display of an appropriate substitute computer location if a match does not exist.

As per claim 30: see Shostack on col.6, lines 58; discusses identifying an appropriate computer to execute a step in either an investigation or a computer security threat response procedure, wherein the computer is strategically located relative to a source of a security incident.

As per claim 31: see Shostack on col.7, lines 55-64; discusses executing one or more program modules in response to a selection of a computer security threat procedure.

As per claim 32: see Shostack on col.7, lines 55-64; discussing one or more program modules comprises one or more software application programs that can operate as a stand-alone programs.

As per claim 33: see Shostack on col.7, lines 55-64; discussing one or more program modules comprises an off the shelf software application programs.

As per claim 34: see Shostack on col.9, lines 58-67; discussing the security incident information comprises predefined attributes.

As per claim 35: see Trcka on col.7, lines 60-63 and col.18, lines 1-14; discussing the predefined attributes comprise any one of a computer incident severity level, a computer incident category, a computer incident scope value, a computer incident status value, an attacker internet protocol (IP) address value, an attacker ISP name, an attacker country, an external attacker status value, an incident type value, a vulnerabilities level, an entry point value, an attack profile value, a target networks value, a target firewalls value, a target hosts value, a target services value, a target accounts value, and a damage type value.

As per claim 36: see Shostack on col.9, lines 58-67; discussing the security incident information comprises attributes that are at least one of variable and computer-generated.

As per claim 37: see Shostack on col.9, lines 58-col.10, line 9; discusses whether a computer security incident comprises an actual breach in security based upon values of its attributes.

As per claim 38: see Shostack on col.6, lines 42-58; discusses receiving a selection for a step of a computer security threat procedure; and generating a pre-execution warning prior to the selection of a step.

As per claim 39: see Shostack on col.6, lines 42-58 and col.7, lines 24-29; discusses receiving a selection for a step of a computer security threat procedure, executing the selected step, and suggesting an appropriate subsequent step in the computer security threat procedure.

As per claim 40: see Shostack on col.11, lines 52-54; discussing each step is performed automatically in response to a detected computer security incident.

As per claim 41: see Shostack on col.12, lines 14-48; discusses providing data to enable display of a plurality of computer tools in a non-procedural manner; receiving a selected for a computer tool; and executing the selected computer tool.

As per claim 42:

Shostack, et al. disclose a method for organizing and recording reactions to one or more security incidents, comprising the steps of:

classifying the computer security incident information; [col.9, lines 59-67]

automatically suggesting one or more computer security threat investigation procedure based on a classification of the computer security incident information; [col.7, lines 25-35 and col.11, lines 52-54]

displaying one or more computer security threat investigation procedures for investigating one of suspicious computer activity [col.7, lines 60-67 and col.12, lines 41-47] that occur prior to a computer security threat and an actual computer security threat; [col.4, lines 50-53]

displaying the one or more computer security threat response procedures for responding to one of suspicious computer activity comprising one or more attacks received from a network computer [col.2, lines 54-56 and col.12, lines 14-25] that occur prior to a computer security threat and an actual computer security threat; [col.7, lines 13-15]

in response to a selection of a computer security threat investigation procedure, providing data to enable display of one or more corresponding investigation steps; [col.7, lines 45-46 and col.8, lines 65-67]

in response to a selection of a computer security threat response procedure, displaying one or more corresponding response steps; [col.2, lines 54-56 and col.12, lines 14-25]

receiving a selection of one or more investigations steps and one or more corresponding response steps; [col.11, lines 49-51and col.12, lines 14-25]

storing a permanent record [col.4, lines 34-35] comprising security incident information, executed investigation step and result information, executed response step and result information [col.7, lines 25-27 and col.13, lines 15-17 and 31-36], and [*corresponding date and time stamp*].

Shostack discusses displaying the one or more suggested computer security threat procedures [col.12, lines 14-25 and 41-47], each computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information [col.6, lines 58 and col.7, lines 25-27]. However, Shostack did not include a date and time stamp and receiving a selection of a suggested computer security threat procedure from a user.

Trcka, et al. discloses an invention that provides a network security and analysis system, which includes a variety of features for automatically and interactively monitoring and analyzing traffic (col.2, lines 11-15 and col.11, lines 1-4). Trcka utilizes archival recordings to evaluate security breaches and other anomalies (col.7, lines 49-

50). The archival recordings can be used to perform a wide range of network analysis and restoration tasks that includes checking for newly discovered viruses and performing low-level analysis of network break-ins (col.2, lines 56-61). Trcka discusses the date/time stamp reflects the dates and times that the packets are transmitted on the network (col.15, lines 55-57). Thus, preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12). Further, the claimed "receiving a selection of a suggested computer security threat procedure from a user, the selection comprising one or more steps of the selected computer security threat procedure", broadly limits a computer security threat procedure that is suggested from a user. This does not limit or define what considers a procedure and security threat involves that can be selected or suggested from a user. The claimed subject matter merely suggests as long as the procedure is computer security threat related. For instance, a selection of a suggest computer security threat procedure from a user can broadly be given in light as security configurations to help prevent or monitor security threats, allowing or not allowing particular traffic or incoming packets, a solution to solve security threat, or specifying types of transactions or filtering parameters. Thus, the following will explain and incorporate these examples found in Trcka. Trcka includes various software routines for monitoring, filtering, searching, and manipulating traffic data and interactive analysis applications which provide functionality for allowing users to interactively analyze and process traffic data (col.12, lines 49-52). In addition, the Automated Monitor application uses known data processing techniques (virus checking, transaction, monitoring, etc.) to automatically check for and track

suspect network events and one configuration option, a user can enable or disable various visual and audible event alarms (col.17, lines 24-32). The user can configure to alert the user when critical limits are exceeded on the network, generate log file of specific types of events, run analysis applications and perform other interactive actions in the foreground (col.17, lines 35-42). The analysis applications provide various functionality for allowing users to interactively perform non-real-time or off line analyses of pre-recorded raw traffic data (col.17, lines 44-50). This shows the user having the ability to interact, which obviously gives instructions to enable a selection of suggested computer security threat procedures in order to receive a selection of suggested computer security threat procedures from a user (col.12, lines 49-52 and col.20, lines 1-17). In addition, Trcka discloses the GUI allows the user to specify the type or types of transactions that are loaded into the databases and/or routed directly to the analysis applications. The types of filtering parameters that can be set by the user include network address, traffic type, packet type, user ID, and packet transaction sequence (col.18, lines 1-14). Trcka discloses the user able to initiate searches of the traffic data at various levels of resolution and search for all packets containing the particular set of source and destination address or for all packets transmitted during a particular time window (col.18, lines 15-52).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of the computer security threat procedure computer based on classification of security incident information as taught by Shostack with the teaching of allowing the user to interactively perform analyses of

traffic data such that the receiving a selection of a suggested computer security threat procedure from a user as taught by Trcka because this allows the user to specify computer security threats procedures such as types of transactions that are loaded into the databases (col.18, lines 1-2 and 40-44), configure to generate a log file of specific types of events (col.17, lines 38-50), and traffic analysis of the particular packets (col.12, lines 49-52 and col.20, lines 1-17). Additionally, it would have been obvious to combine the teaching of recording computer security incident information and the computer security threat procedure as taught by Shostack with at least one of a date and time stamp as taught by Trcka because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

As per claim 43: see Shostack on col.7, lines 24-29 and col.11, lines 50-54; discussing recording executed investigation step information and results of the executed investigation step with at least one of a date and time stamp (Trcka-col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57) in response to a selection of a step of a computer security threat investigation procedure.

As per claim 44: see Shostack on col.7, lines 24-29 and col.13, lines 15-17 and 31-36; discussing recording executed response step information and results of the executed response step with at least one of a date and time stamp (Trcka-col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57) in response to a selection of a step of a computer security threat response procedure.

As per claim 45: see Shostack on col.12, lines 14-48 and col.13, lines 6-17; discusses providing data to enable display of a plurality of a computer security threat procedures; in response to receiving a selection of a computer security threat procedure, displaying a plurality of steps; obtaining modification information for the selected computer security threat procedure; and storing the modification information.

As per claim 46: see Shostack on col.7, lines 24-29; discusses adding or deleting a step in a procedure.

As per claim 47: see Shostack on col.12, lines 14-48 and col.13, lines 6-17; discusses providing data to enable display of a plurality of steps of a computer security threat procedure; in response to receiving a selection of a step, providing data to enable display of detailed information fields related to the selected step; obtaining modification information for the selected step; and storing the modification information.

As per claim 48: see Shostack on col.7, lines 24-29; discusses adding, deleting or modifying a step in a computer security threat procedure.

As per claim 49: see Shostack on col.7, lines 24-29and col.12, lines 14-48; discusses obtaining computer security incident search information and providing data to enable display of a plurality of one or more computer security incidents matching the computer security incident search information.

As per claim 50: see Trcka on col.7, lines 10-12 and col.14, lines 34-36 and col.15, lines 55-57; discusses tracking multiple computer security incidents and storing information for each computer security in accordance with at least one of a date and time stamp.

As per claim 56:

Shostack discloses a method for generating a permanent record or one or more computer security incidents and reactions thereto, comprising the steps of:

receiving the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network [col.4, lines 47-50 and col.5, lines 20-50] that occur prior to a computer security threat [col.7, lines 13-17] and an actual computer security threat; [col.4, lines 50-53]

classifying the computer security incident information; [col.9, lines 59-67]

displaying one or more tools for one of investigating one of suspicious computer activity [col.2, lines 54-56 and col.12, lines 40-48] that occurs prior to a computer security threat [col.7, lines 13-17] and an actual computer security threat; [col.4, lines 50-53]

automatically suggesting one or more tools based on a classification of the computer security incident information; [col.2, lines 36-38 and col.7, lines 23-35 and col.11, lines 50-54]

receiving a selection of a suggested tool; in response to a selection of a tool, forwarding data for execution of the tool; and [col.7, line 55-col.8, line 3 and col.11, lines 49-51]

forwarding data for storing a permanent record comprising computer security incident information, executed tool information [col.7, lines 25-27 and col.13, lines 15-17 and 31-36], and [*corresponding date and time stamp*]

However, Shostack did not include a date and time stamp.

Trcka, et al. discloses an invention that provides a network security and analysis system, which includes a variety of features for automatically and interactively monitoring and analyzing traffic (col.2, lines 11-15 and col.11, lines 1-4). Trcka discloses utilizes archival recordings to evaluate security breaches and other anomalies (col.7, lines 49-50). The archival recordings can be used to perform a wide range of network analysis and restoration tasks that includes checking for newly discovered viruses and performing low-level analysis of network break-ins (col.2, lines 56-61). Further, Trcka discusses the date/time stamp reflects the dates and times that the packets are transmitted on the network (col.15, lines 55-57). Thus, preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of recording computer security incident information and the computer security threat procedure as taught by Shostack with at least one of a date and time stamp as taught by Trcka because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

As per claim 57: see Shostack on col.12, lines 14-48; discusses displaying the tools as icons on a computer display.

As per claim 58: see Shostack on col.12, lines 14-48; discusses displaying a plurality of tools that are selectable from a menu.

As per claim 59: see Shostack on col.10, lines 11-25; discusses installing the one or more program modules within a single program on a server.

As per claim 60: see Shostack on col.10, lines 11-25; discusses installing the one or more program modules on a single server.

As per claim 61: see Shostack on col.11, lines 41-43; discusses installing the one or more program modules on a computer that is a target of a computer incident.

As per claim 62: see Shostack on col.10, lines 11-25; discusses installing the one or more program modules on both a computer that is a target of a computer incident and a server.

As per claim 63: see Trcka on col.7, lines 60-63 and col.18, lines 1-14; discussing comparing an Internet address of a computer subject to an attack or a security breach with the Internet address ranges of the table.

As per claim 64: see Trcka on col.7, lines 60-63 and col.18, lines 1-14; discussing comparing an Internet address of a witness to a computer security incident with the Internet address ranges of the table.

As per claim 65: see Trcka on col.7, lines 60-63 and col.18, lines 1-14; discussing comparing an Internet address of an accomplice to a computer security incident with the Internet address ranges of the table.

NEW GROUND(S) OF REJECTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 51-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack, et al. (US 6,298,445), and further in view of Reps, et al. (US 6,070,190).

As per claim 51:

Shostack, et al. discloses a method for selecting a computer that is strategically located relative to a source of a security incident, comprising the steps of:

the computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity [col.4, lines 47-50 and col.5, lines 20-50] comprising one or more attacks received from a network that occur prior to a computer security threat [col.2, lines 53-56 and col.7, lines 13-17] and an actual computer security threat [col.4, lines 50-53], *[the computer location]* identifying devices that are able to perform the computer security threat procedure; [see col.3, lines 10-33]

comparing a computer security threat procedure to be executed; [col.12, lines 63-65 and col.14, lines 15-30]

determining if a match exists between the computer security step to be executed; [col.7, lines 24-30 and col.12, lines 1-40]

automatically selecting a computer to execute the computer security threat procedure based upon the matching step, and [col.2, lines 35-63 and col.11, lines 52-54]

storing a permanent record [col.9, lines 56-67] comprising the executed computer security threat procedure and result information. [col.11, line 47-col.12, line 10 and col.13, lines 7-35]

Although, Shostack teaches monitoring vulnerabilities and computer security threat procedures, but did not include a table of address ranges, a permanent record with a corresponding date/time stamps, and computer location information or target and Internet address.

Reps discloses a monitoring system should provide dynamic reports where the report should be displayed in a such a manner that the viewer may display either via a graph or table or data relating to the performance of the servers and/or applications (Reps-col.4, lines 47-55). A transaction record includes information related to the performance of the application services where configuration information or parameters includes designations of the remote centralized repositories for forwarding the transaction records (Reps-col.5, lines 24-61). Reps disclose pre-defined performance criteria for the monitored application program that include maximum allowable response time, and/or a maximum number of failed successive attempts to access services of the application program. A determination that one of these pre-defined performance criteria has been violated, prompts to inform an appropriate support entity of the violation such as that problem determination and remediation steps may be implemented (Reps-col.11, lines 15-34). Reps include a target Internet address (Reps-col.11, lines 47-53)

with computer locations and Internet address ranges listed in the table (Reps-col.14, lines 25-67 and col. 25, lines 15-32). Reps discusses accessing a table comprising computer Internet address ranges associated with the computer locations (Reps-col.6, lines 10-30 and col.11, lines 47-53), and computer security threat procedure associated with the computer locations (Reps-col.15, line 42-col.16, line 52). Additionally, Reps discusses comparing and determining if a match exists between an Internet address of a computer security incident and Internet address ranges listed in the table (Reps-col.25, lines 31-37), wherein the computer has a location and is capable of interacting with the Internet address of the security incident (Reps-col.11, lines 23-65 and col.25, lines 39-43), and corresponding date and time stamps (Reps-col.14, lines 1-15).

Therefore it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of computer security threat procedure of Shostack associated with the computer locations (Reps-col.15, line 42-col.16, line 52) of Reps and accessing a table comprising computer Internet address ranges associated with the computer locations (Reps-col.6, lines 10-30 and col.11, lines 47-53), because data should be displayed via a graph or table relating to the performance of servers and/or applications to provide an interactive facility for enabling the viewer to drill down to view data on specific servers or applications and/or to drill up to a broader view of the performance data (Reps-col.4, lines 47-55). Thus, it is further obvious for a person of ordinary skills in the art for a record comprise a corresponding data and time stamps is for keeping track of the transaction as proof of certain activities

(Reps-col.14, lines 1-15) and that accessing a table includes comparing and determining if a match exists (Reps-col.25, lines 31-45).

As per claim 52: see Reps on col.9, lines 24-35; discusses if one or more matches exist, providing data to enable display of the matching information and if a match does not exist, providing data to enable display of one or more appropriate substitute computer location or automatically selecting an appropriate location.

As per claim 53: see Reps on col.16, lines 34-67; discusses a portion of a computer security threat response procedure, wherein the computer is strategically located relative to a source of a security incident.

As per claim 54: see Reps on col.19, lines 27-46; discusses a portion of a computer security threat investigation procedure, wherein the computer is strategically located relative to a source of a security incident.

As per claim 55: see Reps on col.15, lines 7-10; discussing one or more off the shelf security application programs.

(10) Response to Argument

As per arguments to claim 1:

According to appellant's argument on pg.15 (2nd paragraph) of Appeal Brief, *that the GUI of Shostack does not display one or more procedures comprising one or more steps or provide for the reception of a selection of one or more procedures comprising one or more steps.*

First, Shostack discloses in the summary of the invention (col.2, lines 35-39 and 52-58), that the user is able to implement prevention techniques and that a user can request or can be sent automatically when it becomes available a new version of the software enhancement. This reasonably suggests that once the software enhancement is available, the GUI screen displays at least one form of computer threat procedure in order for the user to employ (which is to select) this prevention technique. Shostack then continues to disclose the user can thus obtain instant access to the latest security vulnerabilities and employ immediate remedial action before a security breach occurs (col.2, lines 54-56). It is obvious that a user cannot be a software or an application or a computer because the user employs a prevention action via a GUI screen and cannot electronically execute in code like a software, an application, or computer. Thus, Shostack obviously suggests the one or more steps of responding to the computer security incident. Further, Shostack suggests a push system is manually activated by a user seeking an update (col.7, lines 55-67). Shostack includes checking the operating system by invoking a check operating systems icon on the GUI screen and performs a network scan to assess network security and database of security vulnerabilities by activating the check network icon on the GUI screen (col.12, lines 41-48). This suggests the step of investigating the computer security incident information. Hence, Shostack reads on the claim 1 of displaying one or more suggested computer security threat procedure. Each computer security threat procedure comprising one or more steps of investigating and responding to the computer security incident information.

As for the argument that Shostack does not *provide for the reception of a selection of one or more procedures comprising one or more steps* is traversed because Trcka is combined with Shostack to teach this limitation. Trcka, et al. discloses an invention that provides a network security and analysis system which includes a variety of features for automatically and interactively monitoring and analyzing traffic on a LAN (col.2, lines 11-15 and col.11, lines 1-4 and col.17, lines 44-50). Trcka provides functionality for allowing users to interactively analyze, process traffic data, and manipulate pre-recorded traffic data through a set of powerful analysis tools (col.12, lines 49-52 and col.13, lines 16-19). They include functionality for performing such actions as displaying user specified types of network events, conducting pattern searches, and identifying pre-defined network problems (col.13, lines 20-24). Trcka teaches an Automated Monitor application uses known data processing techniques (virus checking, transaction, monitoring, etc.) to automatically check for and track suspect network event. In one configuration option, a user can enable or disable various visual and audible event alarms upon detecting a virus (col.17, lines 24-35). In addition, Trcka discloses a user configurable filter adjustable via the GUI, which allows the user to efficiently focus on the traffic events of interest (col.17, line 66-col.18, line 14). The types of filtering parameters that can be set by the user including network address, traffic type, packet type, user ID, and packet transaction sequence (col.18, lines 1-14). Trcka discloses the user able to initiate searches of the traffic data at various levels of resolution and search for all packets containing the particular set of source and destination address or for all packets transmitted during a particular time

window (col.18, lines 15-52). Another example, Trcka includes the Audit application presents the user with a set of display screens which allow the user to specify various settings and parameters for selectively viewing and generating audit trails from the archived traffic data and the Problem Determination application allows the user to identify and zoom in on particular types of network problems (col.20, lines 1-35). Trcka also discusses allowing users to interactively reconstruct a specific traffic sequence to recreate error-causing transactions, simulate load conditions, or restore lost or damage files or messages (col.20, lines 44-64). The above shows the user having the ability to interact via a GUI and display screens, which suggests the procedures are displayed to the user, and obviously reads on the claimed receiving a selection of a suggested computer security threat procedure from a user.

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching Shostack with Trcka teaching the receiving a selection of a suggested computer security threat procedure from a user, the selection comprising one or more steps of the selected computer security threat procedure because the user interactively performs analysis of traffic data which allows the user to specify procedures such as filtering parameters (col.18, lines 1-35), configure to generate a log file of specific types of events (col.17, lines 38-50), traffic analysis of the particular packets and to restore lost data or damaged files (col.12, lines 49-52 and col.20, lines 1-63).

Regarding appellant's argument on pg.15 (4th paragraph): *Examiner traverses the argument that Shostack does not provide a teaching of the storage of this type of information. The information is referring to the claimed storing a record comprising the computer security information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, and an identity of a user who selected the computer security threat procedure.*

Appellant agrees Shostack merely provides the storage of the software enhancement that is received and a log of the software enhancement update (see 3rd line from bottom of pg.15). This suggests that Shostack includes a storage for storing the software enhancement. This software enhancement is a form of a result of the executed computer security threat. Thus, Shostack reads on the claimed results of one or more steps of the executed computer security threat (is explained further below). Shostack teaches a database of security vulnerabilities to use the information to provide security solutions to potentially weak computer networks and/or computers (col.4, lines 5-45) and shows TABLE 1 as having information to identify the known threats/vulnerabilities (col.5, line 55-col.6, line 35). This reads on the claimed storing a record comprising the computer security incident information. In addition, Shostack teaches a user can request the enhancement or can be automatically sent when it becomes available where the enhancement can include a new version of the software and an update to a database of known security vulnerabilities (col.2, lines 49-55). The software enhancement is integrated into existing programs and installed when received

by the customer (col.8, lines 19-20 and col.10, lines 11-13). Hence, to integrate or install the software enhancement obviously is to execute and then is stored in the computer. Further, Shostack discusses the push system provides computer security enhancements for execution on at least one computer (col.7, lines 55-57) and the software enhancement is stored on a storage device on the client's computer (col.11, lines 38-40 and col.12, lines 38-40). This reads on the claimed record comprising executed computer security threat procedure and results of one or more steps of the executed computer threat security. Shostack also includes client information obtained from the customer database where the contents of a specified location with the remote server and sends the software enhancement to the client (col.9, lines 16-21). The authenticity and integrity of the software enhancement is determined by verifying digital signatures, authenticating the software, and verifying the user (col.10, lines 21-28). The software enhancement is given a digital signature, which is a function of the message digest number, and the private key where the recipient (user) compares the value obtained from the cryptographic checksum with the value obtained by using the public verification key (col.14, lines 15-29). Thus, the public key is the identity information record of the user who is verified to receive the software enhancement. Therefore, Shostack reads on the claimed record comprising an identity of a user who selected the computer security threat procedure.

Examiner traverses appellant's argument on pg.15 (last paragraph) to pg.16 (2nd paragraph), *that Shostack fails to teach the claimed features of a date and time stamp and receiving a selection of a suggested computer threat procedure.*

Examiner has addressed argument of receiving a selection of a suggested computer threat procedure; please refer above (on pg.28) for the response.

As for Shostack not disclosing the claimed date and time stamp, Trcka is combined with Shostack to teach this limitation. Trcka, et al. discloses an invention that provides a network security and analysis system (col.2, lines 11-15 and col.11, lines 1-4), and utilizes archival recordings to evaluate security breaches and other anomalies (col.7, lines 49-50). Trcka discusses the date/time stamp reflects the dates and times that the packets are transmitted on the network (col.15, lines 55-57). Thus, preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of recording computer security incident information and the computer security threat procedure as taught by Shostack with at least one of a date and time stamp as taught by Trcka because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

As per arguments to claim 42:

Appellant's arguments on pg.17 (2nd paragraph) are noted with respect to claim 1, *that Shostack does not teach the claimed features of a date and time stamp and receiving a selection of a suggested computer threat procedure. Examiner also traverses the argument where Shostack or Trcka suggest the storing a permanent record comprising computer security incident information, executed investigation step and result information, and executed response step and result information.*

Shostack does not include a date and time stamp, thus, is combined with Trcka to teach this limitation. Trcka discloses the date/time stamp reflects the dates and times that the packets are transmitted on the network (col.15, lines 55-57), to preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12). Thus, it would have been obvious for a person of ordinary skills to combine the teaching of Shostack with Trcka to teach at least one of a date and time stamp because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

Further, Shostack is combined with Trcka to teach receiving a selection of a suggested computer threat procedure is addressed above on pg.28.

As for the argument regarding the permanent record: Shostack teaches a database of security vulnerabilities to use the information to provide security solutions to potentially weak computer networks and/or computers (col.4, lines 5-45) and shows TABLE 1 as having information to identify the known threats/vulnerabilities (col.5, line

55-col.6, line 35). This reads on the claimed storing a record comprising the computer security incident information. Shostack teaches a user can request the enhancement or can be automatically sent when it becomes available where the enhancement can include a new version of the software and an update to a database of known security vulnerabilities (col.2, lines 49-55). The software enhancement is integrated into existing programs and installed when received by the customer (col.8, lines 19-20 and col.10, lines 11-13). Hence, to integrate or install the software enhancement obviously is to execute and stored in the computer. Further, Shostack discusses the push system provides computer security enhancements for execution on at least one computer (col.7, lines 55-57) and the software enhancement is stored on a storage device on the client's computer (col.11, lines 38-40 and col.12, lines 38-40). This reads on the claimed record comprising executed computer security threat procedure and results of one or more steps of the executed computer threat security. Shostack also includes client information obtained from the customer database where the contents of a specified location with the remote server and sends the software enhancement to the client (col.9, lines 16-21). The authenticity and integrity of the software enhancement is determined by verifying digital signatures, authenticating the software, and verifying the user (col.10, lines 21-28). The software enhancement is given a digital signature, which is a function of the message digest number, and the private key where the recipient (user) compares the value obtained from the cryptographic checksum with the value obtained by using the public verification key (col.14, lines 15-29). The public key is the identity information record of the user who is verified to receive the software

enhancement. Thus, this suggests claimed record comprising an identity of a user who selected the computer security threat procedure. Therefore, Shostack reads on the claimed permanent record.

As per arguments to claim 51:

Regarding appellant's arguments on pg.20 (1st paragraph): Appellant argues that Reps does not provide any teaching of a computer security threat procedure comprising one or more steps of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat and executing a computer security threat procedure.

Claims 51-55 are now rejected as being unpatentable over Shostack in view of Reps.

Reps discloses problem determination and remediation steps for violations to access services of the application program (Reps- col.4, lines 47-55 and col.11, lines 15-34). Reps do not suggest the violations or computer security threats of a computer security system. Shostack is the primary reference that teaches computer security threats or attacks and executing computer security threat procedure for computer networks and/or computers (Shostack-col.4, lines 5-45).

Shostack teaches a database of security vulnerabilities to use the information to provide security solutions to potentially weak computer networks and/or computers (col.4, lines 5-45) and shows TABLE 1 as having information what to look for to identify

the known threats/vulnerabilities (col.5, line 55-col.6, line 35). Shostack teaches a user can request the enhancement or can be automatically sent when it becomes available where the enhancement can include a new version of the software and an update to a database of known security vulnerabilities (col.2, lines 49-55). The software enhancement is integrated into existing programs and installed when received by the customer (col.8, lines 19-20 and col.10, lines 11-13). Shostack discusses the push system provides computer security enhancements for execution on at least one computer (col.7, lines 55-57) and the software enhancement is stored on a storage device on the client's computer (col.11, lines 38-40 and col.12, lines 38-40). Further, Shostack also includes client information is obtained from the customer database where the contents of a specified location with the remote server and sends the software enhancement to the client (col.9, lines 16-21). The authenticity and integrity of the software enhancement is determined by verifying digital signatures, authenticating the software, and verifying the user (col.10, lines 21-28). Hence, Shostack teaches the claimed computer security threat procedure comprising one or more steps for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat.

Regarding appellant's arguments on pg.20 (3rd paragraph): *Appellant argues that Reps and Shostack do not teach accessing a table comprising computer locations,*

Internet address ranges associated with the computer locations, and computer security threat procedure associated with the computer locations.

Shostack teaches monitoring vulnerabilities and computer security threat procedures, but did not include a table comprising Internet addresses ranges or locations and date/time stamp. Shostack is combined with Reps to teach a table of address ranges, computer location information or target, and Internet address.

Reps discloses a monitoring system should provide dynamic reports where the report should be displayed in a such a manner that the viewer may display either via a graph or table or data relating to the performance of the servers and/or applications (Reps-col.4, lines 47-55). Reps include a target Internet address (Reps-col.11, lines 47-53) with computer locations and Internet address ranges listed in the table (Reps-col.14, lines 25-67 and col. 25, lines 15-32). Reps discusses accessing a table comprising computer Internet address ranges associated with the computer locations (Reps-col.6, lines 10-30 and col.11, lines 47-53), and computer security threat procedure associated with the computer locations (Reps-col.15, line 42-col.16, line 52). Additionally, Reps discusses comparing and determining if a match exists between an Internet address of a computer security incident and Internet address ranges listed in the table (Reps-col.25, lines 31-37), wherein the computer has a location and is capable of interacting with the Internet address of the security incident (Reps-col.11, lines 23-65 and col.25, lines 39-43).

Therefore it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of computer security threat

procedure of Shostack associated with the computer locations (Reps-col.15, line 42-col.16, line 52) of Reps and accessing a table comprising computer Internet address ranges associated with the computer locations (Reps-col.6, lines 10-30 and col.11, lines 47-53), because data should be displayed via a graph or table relating to the performance of servers and/or applications to provide an interactive facility for enabling the viewer to drill down to view data on specific servers or applications and/or to drill up to a broader view of the performance data (Reps-col.4, lines 47-55).

Regarding appellant's arguments on pg.21: *Appellant argues neither Reps nor Shostack provide storing a permanent record comprising the executed computer security threat procedure, result information, and corresponding date and time stamp.*

Shostack teaches a database of security vulnerabilities to use the information to provide security solutions to potentially weak computer networks and/or computers (col.4, lines 5-45). Shostack teaches a user can request the enhancement or can be automatically sent when it becomes available where the enhancement can include a new version of the software and an update to a database of known security vulnerabilities (col.2, lines 49-55). The software enhancement is integrated into existing programs and installed when received by the customer (col.8, lines 19-20 and col.10, lines 11-13). Hence, to integrate or install the software enhancement obviously is to execute and stored in the computer. Further, Shostack discusses the push system provides computer security enhancements for execution on at least one computer (col.7, lines 55-57) and the software enhancement is stored on a storage device on the

client's computer (col.11, lines 38-40 and col.12, lines 38-40). This reads on the claimed record comprising executed computer security threat procedure and results of one or more steps of the executed computer threat security. Therefore, Shostack reads on the claimed permanent record comprising the executed computer security threat procedure and result information. As for the corresponding date and time stamp, Reps suggest this limitation.

Reps include a timer mechanism (date/time stamps), which places a time signature for the transaction records (Reps-col.14, lines 1-15). Thus, it is obvious for a person of ordinary skills in the art for a record comprise a corresponding data and time stamp is for keeping track of the transaction as proof of certain activities (Reps-col.14, lines 1-15) and that accessing a table includes comparing and determining if a match exists (Reps-col.25, lines 31-45).

As per arguments to claim 56:

Regarding appellant's arguments on pg.22 (2nd paragraph): Shostack does not teach the feature of a date and time stamp and that Shostack in combination with Trcka does not render obvious.

Trcka is indeed relied upon to teach the feature of a date and time stamp. Trcka, et al. discloses an invention that provides a network security and analysis system (col.2, lines 11-15 and col.11, lines 1-4), and utilizes archival recordings to evaluate security breaches and other anomalies (col.7, lines 49-50). Trcka discusses the date/time stamp reflects the dates and times that the packets are transmitted on the network

(col.15, lines 55-57). Thus, preserve the details of the original timing of the traffic on the network and to facilitate the subsequent reconstruction of network events (col.7, lines 10-12). Therefore, it would have been obvious for a person of ordinary skills in the art combine the teaching of Shostack with Trcka to teach the feature of a date and time stamp because this preserves the original timing of the traffic on the network and facilitates subsequent reconstruction of network events (col.7, lines 10-12 and col.14, lines 34-36).

As per arguments to dependent claims 2-9, 11-41, 43-50, 52-55, and 57-65:

All dependent claims, they are also rejected by virtue of their dependency.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

This examiner's answer contains a new ground of rejection set forth in section (9) above. Accordingly, appellant must within **TWO MONTHS** from the date of this answer exercise one of the following two options to avoid *sua sponte* **dismissal of the appeal** as to the claims subject to the new ground of rejection:

(1) **Reopen prosecution.** Request that prosecution be reopened before the primary examiner by filing a reply under 37 CFR 1.111 with or without amendment, affidavit or other evidence. Any amendment, affidavit or other evidence must be

relevant to the new grounds of rejection. A request that complies with 37 CFR 41.39(b)(1) will be entered and considered. Any request that prosecution be reopened will be treated as a request to withdraw the appeal.

(2) **Maintain appeal.** Request that the appeal be maintained by filing a reply brief as set forth in 37 CFR 41.41. Such a reply brief must address each new ground of rejection as set forth in 37 CFR 41.37(c)(1)(vii) and should be in compliance with the other requirements of 37 CFR 41.37(c). If a reply brief filed pursuant to 37 CFR 41.39(b)(2) is accompanied by any amendment, affidavit or other evidence, it shall be treated as a request that prosecution be reopened before the primary examiner under 37 CFR 41.39(b)(1).

Extensions of time under 37 CFR 1.136(a) are not applicable to the TWO MONTH time period set forth above. See 37 CFR 1.136(b) for extensions of time to reply for patent applications and 37 CFR 1.550(c) for extensions of time to reply for ex parte reexamination proceedings.

A Technology Center Director or designee must personally approve the new ground(s) of rejection set forth in section (9) above by signing below:

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Leynna Ha LH

Conferees:

Kim Vu

Hosuk Song

JAMES DWYER, DIRECTOR
TECHNOLOGY CENTER 2100

KING & SPALDING LLP
1180 Peachtree Street

34th Floor

Atlanta, GA 30309

(404) 572-4600 (Telephone)
(404) 572-5134 (Facsimile)